Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

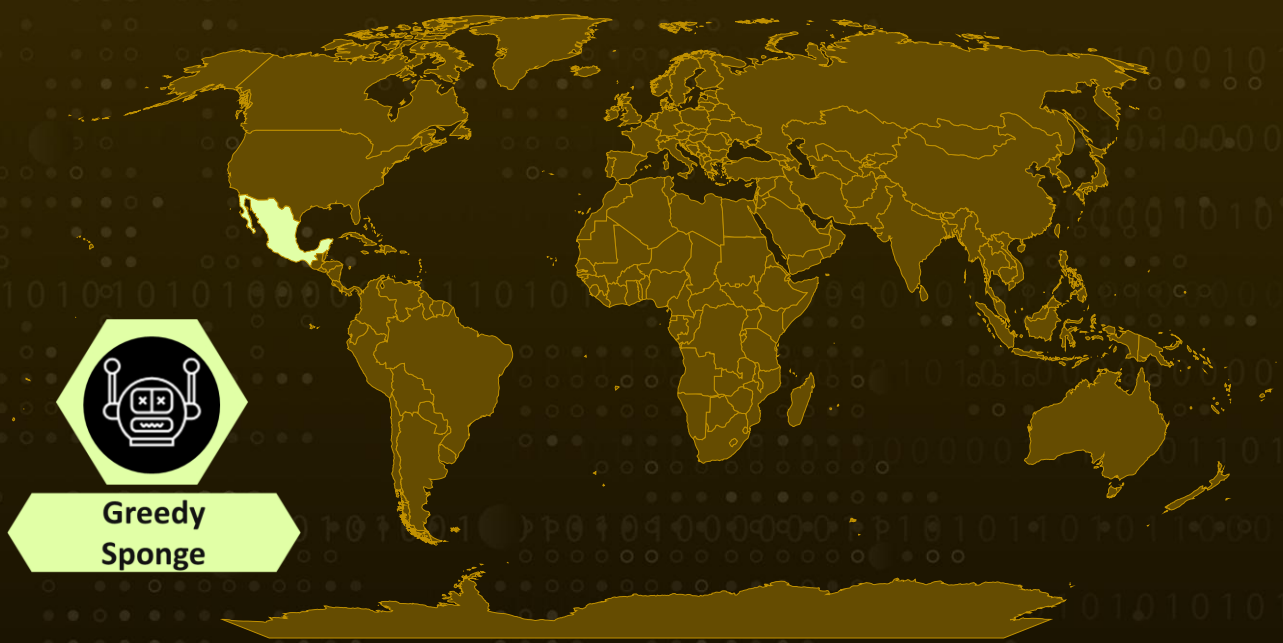
Greedy Sponge's Stealthy RAT Attack in Mexico

Date of Publication	Admiralty Code	TA Number
July 25, 2025	A1	TA2025231

Summary

Attack Discovered: Mid 2024
Targeted Country: Mexico
Malware: AllaKore RAT, SystemBC
Actor: Greedy Sponge
Attack: A financially motivated cybercriminal group known as Greedy Sponge has been actively targeting organizations across Mexico using customized versions of the AllaKore remote access trojan (RAT). Their goal is to steal financial data to commit fraud. By delivering the malware through convincing phishing campaigns often disguised as policy updates or business-related files, they trick victims into installing malicious software. Once inside, the attackers not only steal valuable data but also deploy SystemBC, a secondary malware. Over time, the group has fine-tuned its tactics, improved its targeting of Mexican companies, and enhanced its evasion techniques. Their continued evolution and deliberate focus on the region underscore a persistent and growing threat to organizations in Mexico.

Attack Regions



Attack Details

#1 A financially motivated threat actor known as Greedy Sponge has been persistently targeting organizations across Mexico, with campaigns that have steadily evolved since 2021. The group specializes in financial fraud, using highly customized versions of the open-source AllaKore Remote Access Trojan (RAT) to steal banking credentials and authentication tokens. These modified RATs are designed to send sensitive financial information directly to their command-and-control (C2) infrastructure, enabling targeted banking fraud.

#2 Greedy Sponge typically initiates attacks through phishing emails and fake websites that mimic legitimate Mexican business portals. Their lures and file names such as “InstalarActualiza_Policy.msi” are crafted in Spanish to blend into the local business ecosystem. The initial infection often arrives as a ZIP archive containing a trojanized MSI installer and a Chrome proxy executable. Upon execution, these drop a modified AllaKore RAT and, in some cases, SystemBC a stealthy, multiplatform malware proxy that aids in evading detection and maintaining long-term access.

#3 The RAT is capable of full system control, keylogging, taking screenshots, transferring files, and executing remote commands. It persists by downloading updates from a hidden URI and placing them in the Windows Startup folder. Secondary payloads are dropped into the AppData directory and launched immediately. These samples also feature internal code tailored to capture updated banking site authentication mechanisms, indicating a direct focus on real-time credential theft and token hijacking.

#4 One notable addition to their attack chain is the use of CMSTP-based UAC bypasses, leveraging Microsoft's Connection Manager Profile Installer to execute malware with elevated privileges. This red teaming-style technique, combined with steady improvements to delivery and post-exploitation, signals an increasingly sophisticated threat actor.

#5 Infrastructure-wise, Greedy Sponge hosts its servers with Hostwinds in Dallas, Texas strategically close to Mexico but beyond direct jurisdiction of local law enforcement. Their malware uses a distinctive .NET downloader with a spoofed “Mozilla/4.0” user-agent and operates from hardcoded IPs. Their activities reflect not only financial motivation but also a deep familiarity with the Mexican regulatory landscape, local economic targets, and the Spanish language.

#6 Over the years, Greedy Sponge has transformed from a group deploying open-source RATs into a threat actor with custom-built malware, geofenced targeting, and layered infection strategies making them a notable and persistent risk to organizations operating in Mexico.

Recommendations

- **Be cautious with unexpected files:** Don't open or install files from emails or websites unless you're absolutely sure they're safe even if the file name looks professional or familiar. Threat actors often disguise malware as legitimate business documents.
- **Keep systems and software updated:** Regularly apply updates and patches to your operating systems, browsers, and software. Outdated software often has security holes that attackers exploit.
- **Monitor for unusual behavior:** Keep an eye out for strange system activity, like unknown programs running, increased CPU usage, or attempts to connect to unfamiliar external servers. These could be signs of malware at work.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0004 Privilege Escalation	**TA0005** Defense Evasion	**TA0006** Credential Access	**TA0009** Collection
TA0010 Exfiltration	**TA0011** Command and Control	**T1591** Gather Victim Org Information	**T1591.001** Determine Physical Locations
T1027 Obfuscated Files or Information	**T1027.015** Compression	**T1218** System Binary Proxy Execution	**T1218.007** Msiexec
T1204 User Execution	**T1204.002** Malicious File	**T1105** Ingress Tool Transfer	**T1059** Command and Scripting Interpreter

T1059.005 Visual Basic	T1070 Indicator Removal	T1070.004 File Deletion	T1132 Data Encoding
T1132.001 Standard Encoding	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1140 Deobfuscate/Decode Files or Information
T1056 Input Capture	T1056.001 Keylogging	T1113 Screen Capture	T1547 Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	T1041 Exfiltration Over C2 Channel	T1555 Credentials from Password Stores	T1548 Abuse Elevation Control Mechanism
T1548.002 Bypass User Account Control	T1218 System Binary Proxy Execution	T1218.003 CMSTP	T1566 Phishing
T1566.001 Spearphishing Attachment	T1059.001 PowerShell		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	20fe630a63dd1741ec4ade9fe05b2e7e57208f776d5e20bbf0a012fea96ad0c0, f76b456cf2af1382325c704bf70b5168d28d30da0f3d0a5207901277e01db395, 4bf4bcf1cc45d9e50efbd184aad827e2c81f900a53961cf4fbea90fa31ca7549, fed1c094280d1361e8a9aafdb4c1b3e63e0f2e5bb549d5d737d0a33f2b63b4b8, 5d16547900119112c12a755e099bed1fafe1890869df4db297a6a21ec40185b0, e9cd7c4db074c8e7c6b488a724be1cd05c8536dae28674ce3aa48ebb258e3c31, 32ef3a0da762bc88afb876537809350a885bbbc3ec59b1838e9e9ccc0a04b081, d8343068669d8fbb52b0af87bd3d4f3579d76192d021b37b6fd236b0973e4a5d,

TYPE	VALUE
SHA256	53b85d1b7127c365a4ebae5f22ed479cd5d7e9efc716fb9df68ebdd18551834a, 84b046a4dbfcd9d4b2d62b4bc8faaf4c6395696f1e688f464bc9e0b760885263, 50e5cd438024b34ba638e170f6e4595b0361dedb0ea925d06d06f68988468ddf, 9170503615e4d2cf1d67f0935ded3ce36a984247ae7f9ab406d81ebe1daf3604, c3e7089e47e5c9fc896214bc44d35608854cd5fa70ae5c19aadb0748c6b353d6, 8bf0d693033a761843ae20c7e118c05f851230cb95058f836ffe2b51770f788a, a83f218d9dbb05c1808a71c75f3535551b67d41da6bb027ac0972597a1fc49fe, 21614973732d4012889da2e1538b20fd1c0aefdb1d1452d79fd9a1bc06d569da, a8abffa5d7259a94951d96ad3d60e8910927b5d0697f8edece2e295154e00832, 12557dcf9c9a609521d7a2cc84a7e6fb95a93957aed6bda0f9644e96dfbbc180, dcfa26a38a5af8a072104854fba1b7c0aa9ec99875d35dbd623c12932df44969, bd299b5e3d7645b10286410f98f6ec79d803ce2b977c61e49f2dc26285823c99, 681b15a43925e02d7f4f0c9e554e8d73e230931ce6634f49dd5b204afd03d20c, e9b9cdb713bfea40e13acffbe90faa536df206675819035835ce9218365cd118, 65fc84ffd9be05720b700292b7dbc0ac8afa7faaadf6fcd4485ce34785ba0932, 3b0772608844821555bb90e0218972f89f421dad9b1f7bd1918de26a929e998f, bb3f433799c30a8aad5257abc2df479ecad058f6099fd89fb8e7c278dfe3be45, 34e347d1c9ce80b4e2b77f2de5aa7b4d98084704896bd169338c6d4b440e16c3, 5b51d1682cbd40cc6eca23333554ab16b7ed4bbd727712b3a00b07c24e629863, 544091acb5807aaac32ca4843bb85c4aa7ce0ab0acda296efa1a23fe3c181b7e, 8634988a90e69d8e657f72cf5f599176be5854448e0544abc42eb49b0c245f0c, 79a5ac15d0de66df3dd00a4148aa76dc183ebf47553fbcc5355f4902dc981267, dc409e9fa8b8c031c347d9c36f5732ea03e246c29d73e3425e4e8aaa1da6ff7c,

TYPE	VALUE
SHA256	f5adef8c202e62125be49f748ed3b30b34e0fb2c9539c805dd96a75a26c7ddc4, c33723a6c0ece4f790396f5fd5133cf384143736e6acd06e1d7642c04757bbae, e4a6be2fb70603f1545641240680b44e21b5601e8016c0d144711423eef9778e, 0dbaf8970c0620e1b5902fd87c1cd0e72e917c45add84a024338c0481b5e161c, e848a0f1900e2f0be9ed1ea8e947ae3bae14e78f3ff81c02d8e5a54353cdbac8, b9bb43b725a454e826ab64fdd6256af809c60119dab2876d081b3721d226c672, 3729396b11c69c60f9d096ce726f4cc5b4ed2054d89f7d195e998456de7fb229, 73a46441a7135296d1070f5905a5cb6453ea8511a99a3b9c76060069aa7abcef, 974c221c75c35d03dd2158d1d1a0a72a7ae85a6f7c1c729977f3676f946758ee
Domains	glossovers[.]com, logisticasmata[.]com, inmobiliariaarte[.]com, mx-terrasabvia[.]com, elitesubmissions[.]com, pasaaportes-citas-srre-gob[.]com, arimateas[.]com, cleanmades[.]com, capitolioeventos[.]com, pachisuave[.]com, manzisuape[.]com, siperasul[.]com, cupertujo[.]com, idaculipa[.]com, mepunico[.]com, barrosuon[.]com, tlelmeuas[.]com, trenipono[.]com, kalichepa[.]com, metritono[.]com, masamadreartesanal[.]com
MD5	35932f5856dbf8ba51e048b3b2bb2d7b, 63a5bc24837a392bc56de93b28c7d011, 42300099a726353abfddbfdd5773de83, ac2fa680544b1b1e452753b78b460a59

TYPE	VALUE
Filename	Actualiza_Policy_v01.zip, chrome_proxy.exe, Gadget.exe, Tweaker.exe, kgm.exe, chancla.exe, ChromeUpd.exe
IPv4	254[.]133[.]54, 11.[1]99[.]35, 142[.]11[.]199[.]35

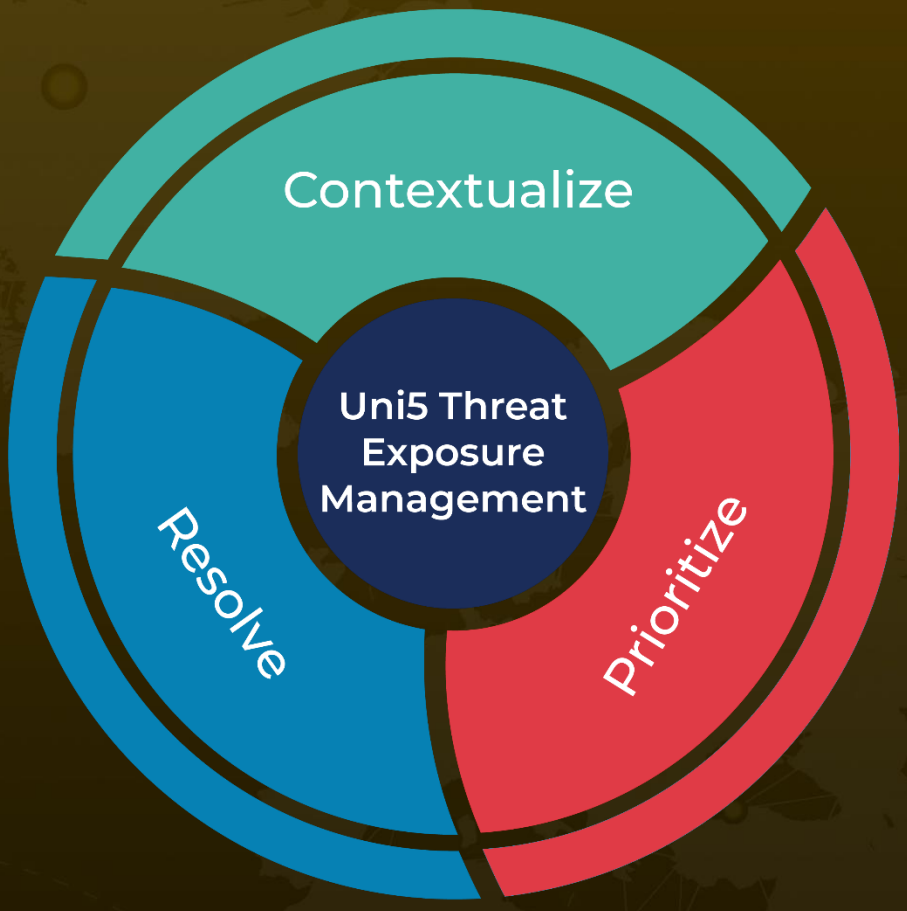
References

https://arcticwolf.com/resources/blog/greedy-sponge-targets-mexico-with-allakore-rat-and-systembc/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 25, 2025 • 7:00 AM

More at www.hivepro.com